WHAT IS CLAIMED IS:

1. A packet processing method comprising:

receiving a plurality of packets;

generating header information for the packets;

adding the header information to the packets to generate encapsulated packets; and

distributing the encapsulated packets to a plurality of encryption processors.

2. The method of claim 1 wherein the information comprises one or more of the group consisting of sequence number and byte count.

3. The method of claim 1 wherein the encapsulated packets comprise IPsec packets.

4. The method of claim 1 wherein packets are encapsulated on a per-packet basis.

5. The method of claim 1 wherein the packets are not encapsulated using parallel processing.

6. The method of claim 1 wherein the packets are received from a host processor.

7. A packet processing method comprising:

receiving a plurality of packets;

identifying security association information associated with the packets;

retrieving the security association information from a data memory;

modifying at least a portion of the security association information;

adding header information to the packets to generate encapsulated packets, wherein the header information comprises the modified at least a portion of the security association information; and

distributing the encapsulated packets to a plurality of encryption processors.

8. The method of claim 7 wherein the at least a portion of the security association information comprises one or more of the group consisting of sequence number and byte count.

9. The method of claim 8 wherein a byte count retrieved from the data memory is modified by adding a length of an outer IP header and a security header.

10. The method of claim 7 wherein the encapsulated packets comprise IPsec packets.

11. The method of claim 7 wherein packets are encapsulated on a per-packet basis.

12. The method of claim 7 wherein the packets are not encapsulated using parallel processing.

13. The method of claim 7 wherein the packets are received from a host processor.

14. A packet processing method comprising:

receiving a plurality of encrypted packets comprising header information;

distributing the encrypted packets to a plurality of decryption processors;

modifying, by a common processing component, at least a portion of the header information of the decrypted packets; and

transmitting the decrypted packets.

15. The method of claim 14 wherein the at least a portion of the header information comprises one or more of the group consisting of sequence number and byte count.

16. The method of claim 14 wherein the encrypted packets comprise IPsec packets.

17. The method of claim 14 wherein the at least a portion of the header information is modified on a per-packet basis.

18. The method of claim 14 wherein the at least a portion of the header information is not modified using parallel processing.

19. The method of claim 14 wherein the packets are transmitted to a host processor.

20. A packet processing method comprising:

receiving a plurality of encrypted packets;

identifying security association information associated with the packets;

distributing the encrypted packets to a plurality of decryption processors to generate decrypted packets;

modifying, by a common processing component, at least a portion of the security association information; and

transmitting the decrypted packets comprising the modified security association information.

21. The method of claim 20 wherein the at least a portion of the security association information comprises one or more of the group consisting of sequence number and byte count.

22. The method of claim 20 wherein the encrypted packets comprise IPsec packets.

23. The method of claim 20 further comprising:

retrieving a first portion of the security association information from at least one data memory; and

distributing the first portion of the security association information to the plurality of decryption processors.

24. The method of claim 20 wherein the at least a portion of the security association information comprises at least one address associated with at least one updateable field in the security association information, the method further comprising:

retrieving the at least a portion of the security association information from at least one data memory; and

distributing the at least a portion of the security association information to the plurality of decryption processors; and

retrieving, according to the at least a portion of the security association information, the at least one updateable field from the at least one data memory.

25. The method of claim 20 wherein the at least a portion of the security association information associated with the packets is modified on a per-packet basis.

26. The method of claim 20 wherein the at least a portion of the security association information associated with the packets is not modified using parallel processing.

27. The method of claim 20 wherein the decrypted packets are transmitted to a host processor.

28. A packet processing system comprising:

at least one media access controller for receiving a plurality of packets;

at least one data memory for storing security association information;

a header processor for modifying at least a portion of the security association information and adding header information to the packets to generate encapsulated packets, wherein the header information comprises the modified at least a portion of the security association information; and

a plurality of encryption processors for encrypting the encapsulated packets.

29. The packet processing system of claim 28 wherein the at least a portion of the security association information comprises one or more of the group consisting of sequence number and byte count.

30. A packet processing system comprising:

at least one media access controller for receiving a plurality of encrypted packets;

at least one data memory for storing security association information;

a plurality of decryption processors for decrypting the encrypted packets to generate decrypted packets;

a header processor for modifying at least a portion of the security association information and modifying header information for the decrypted packets, wherein the header information comprises the modified at least a portion of the security association information.

31. The packet processing system of claim 30 wherein the at least a portion of the security association information comprises one or more of the group consisting of sequence number and byte count.